Cyber Security Requirements Methodology: Tools & Transition

Sponsor: OUSD(R&E) | CCDC AC [WRT-1013]

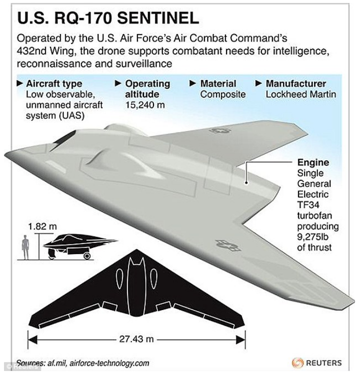
By
Peter Beling and Tim Sherburne
Barry Horowitz, Cody Fleming, Stephen Adams, Giorgos Bakirtzis

11th Annual SERC Sponsor Research Review
November 19, 2019
FHI 360 CONFERENCE CENTER
1825 Connecticut Avenue NW, 8th Floor
Washington, DC 20009

www.sercuarc.org

Cyber Attacks on CPS

Stuxnet 2010



U.S. RQ-170 SENTINEL

Operated by the U.S. Air Force's Air Combat Command's 432nd Wing, the drone supports combatant needs for intelligence, reconnaissance and surveillance

- Aircraft type: Low observable, unmanned aircraft system (UAS)
- Operating altitude: 15,240 m
- Material: Composite
- Manufacturer: Lockheed Martin

Engine: Single General Electric TF34 turbofan producing 9,275lb of thrust

Sources: af.mil, airforce-technology.com

REUTERS

Drone Capture 2011

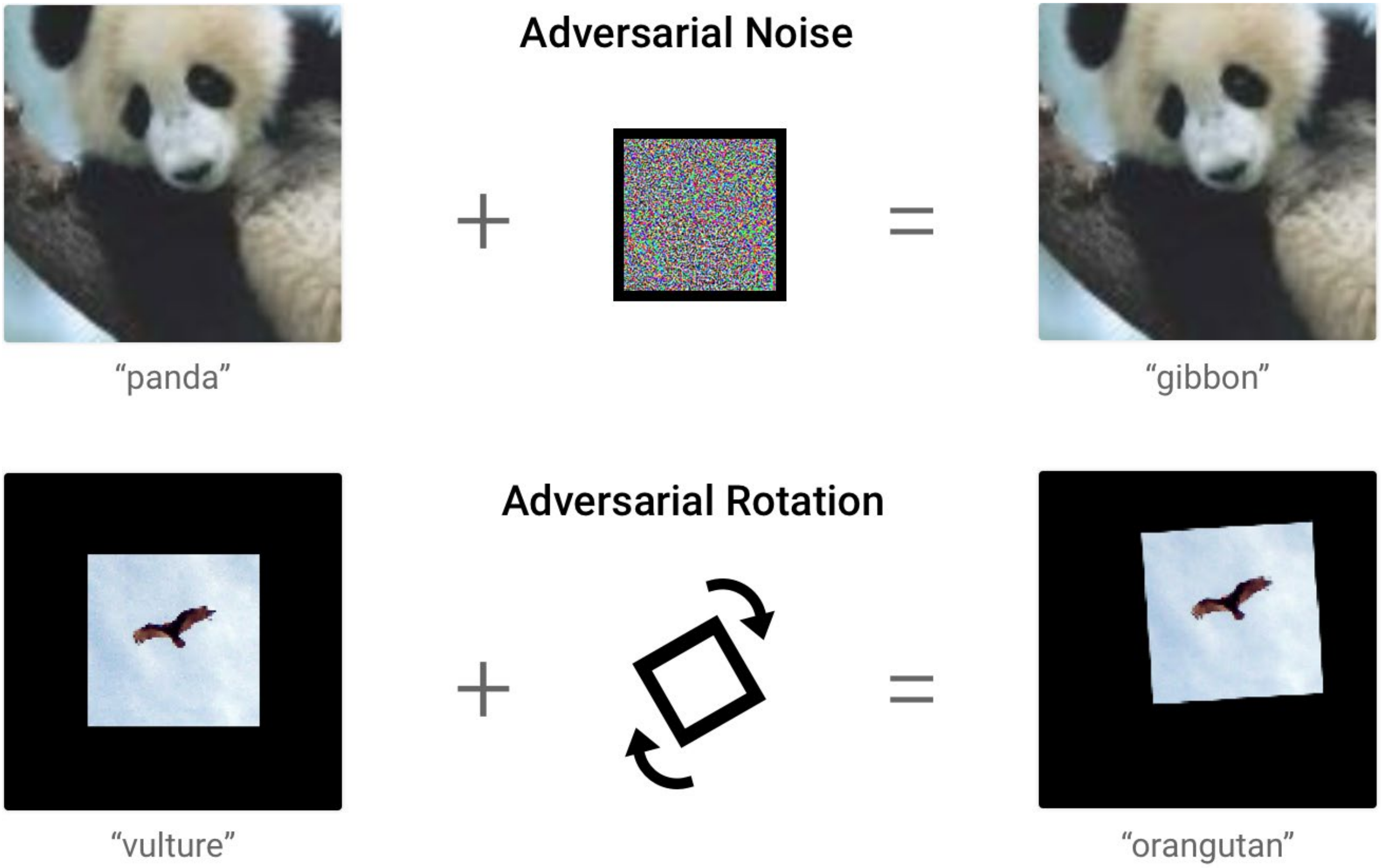
Remote Vehicle Hacks 2015

Chemical Plant 2017

Lab Demonstrations

Sponsor: DoD (OSD, Army, Air Force)

Adversarial Attacks on AI



Adversarial Noise

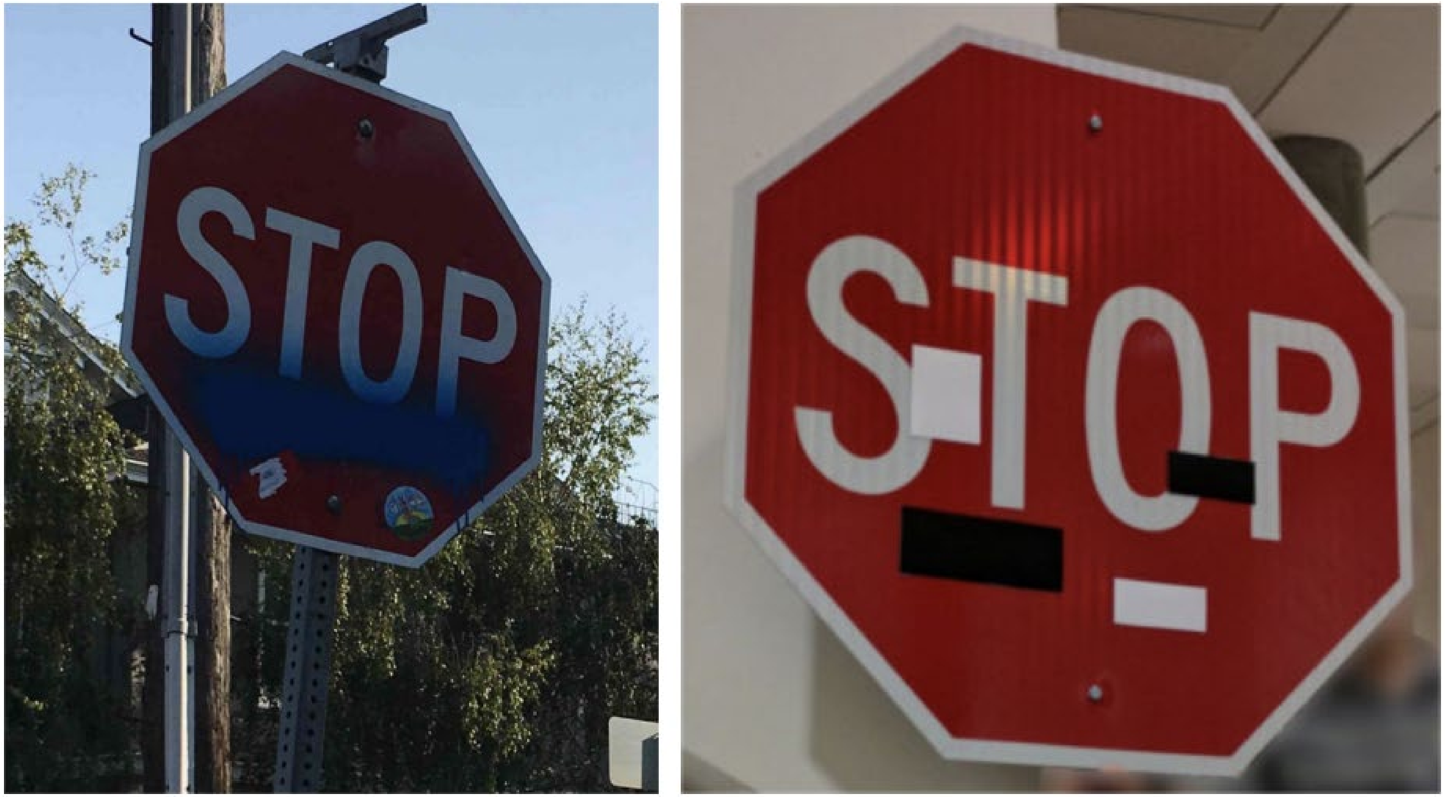
"panda" + = "gibbon"

Adversarial Rotation

"vulture" + = "orangutan"

Source: Google

No Hacking Needed!



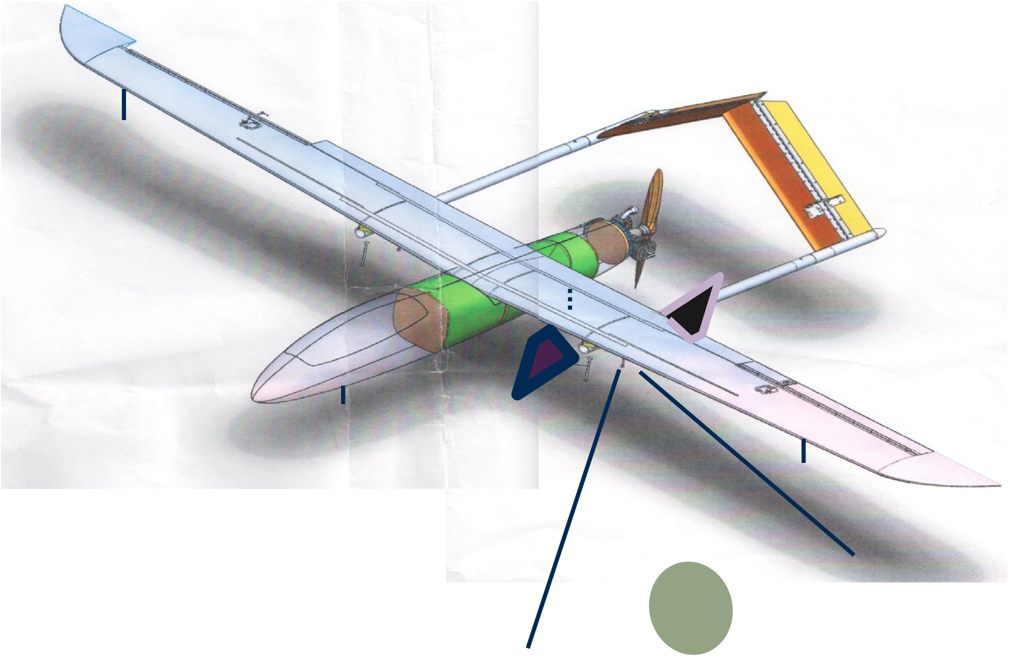
Eykholt, Kevin, et al. "Robust physical-world attacks on deep learning models." *arXiv preprint arXiv:1707.08945* (2017).

Engineering Cyber Resilience

Cybersecurity?–No!
- Physical points of entry
- Off-the-shelf electronics
- Insider threat

Deterrence:
- Reverse asymmetry; erode attacker confidence
- Minimize changes to the system while maximizing uncertainty for the attacker

Resilience:
- Ensure acceptable mission outcome
- Condition on certainty of attack.
- “Point defense rather than perimeter defense.”

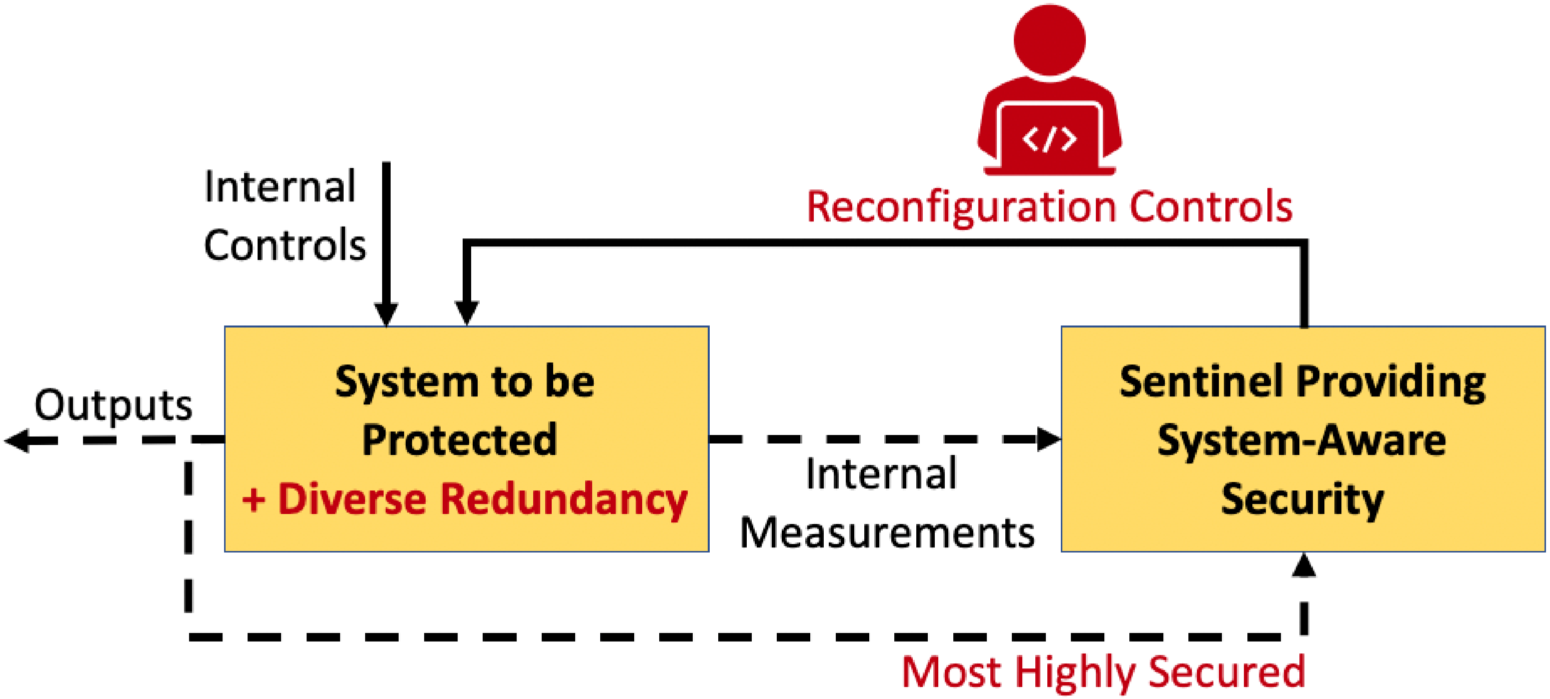


GAUSS Surveillance UAV

Approach:
1. Identify nightmare scenario
   - GPS compromise
2. Behavior-based detection mechanism
   - Voting between two GPS units
3. Switch operating mode
   - Mission termination

Resilience-focused System Architectures and Reusable SW Design Patterns

High Level Architectural Overview



System Resilience*

- Resilience - the capacity of a system to maintain state awareness (implies a monitoring process) and to proactively maintain a safe level of operational normalcy in response to anomalies (implies a process of system reconfiguration, based upon diverse redundancy), including threats of a malicious and unexpected nature.

- The required anticipatory processes for monitoring and reconfiguration is conducted by a subsystem referred to as a **Sentinel**, which should be far more secure than the system being addressed for resiliency

- While the cyber attack detection process is expected to be automated, the level of reconfiguration automation may vary across system functions:
  - Totally Automated (Sentinel determines what to do and informs appropriately trained system operators regarding automated execution)
  - Semi-automated (System operators receive automated recommendation(s) from Sentinel and, accounting for both battle context and a broader set of information available to them, decide on what to do)
  - Manual (Operators, or higher levels in the command hierarchy, determine what to do)

- In addition, resilience includes:
  - Containing the immediate consequences of the detected attack
  - Post-attack forensic support based upon the data collected for addressing anomalies.

Black Text: Rieger, etal, 2009 IEEE Human System Interactions Conference
Red Text: Related to Cyber Attack Resiliency: B.M Horowitz, UVA

Examples of Reusable Design Patterns That Have Been Prototyped

- **Diverse Redundancy** for post-attack restoration
- **Diverse Redundancy + Verifiable Voting** for trans-attack attack deflection
- **Physical and Virtual Configuration Hopping** for moving target defense
- **Data Consistency Checking** for data integrity and operator display protection
- **Parameter Assurance** for parameter controlled SW functions
- **Application-Layer Introspection** for matching machine work loads to observed system behavior
- **Real-time Resilience Testing** for increased operator confidence

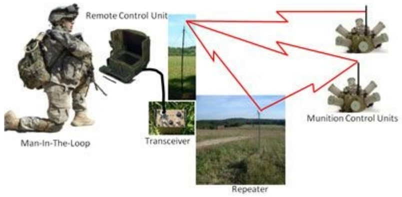
UVA Cyber Resilience Group

Beling, Fleming, Horowitz

Ship Control
(Northrop Grumman)

3D Printers
(NIST)

Human Factors Experiments
(RT-201, Air Force)



Networked Munitions
(RT-191/196, Army)

Cars
(VA State Police)

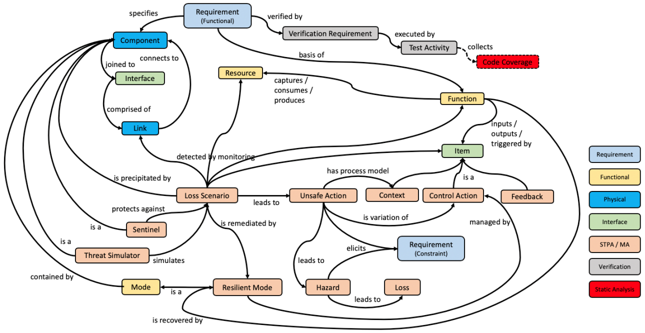
Industrial Control Systems
(Mission Secure Inc)

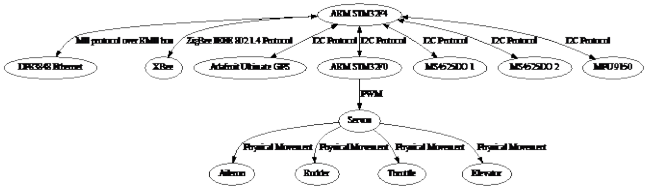
Risk-Based Cyber Security Requirements Methodology

Decision Support for Design for Cyber Resilience

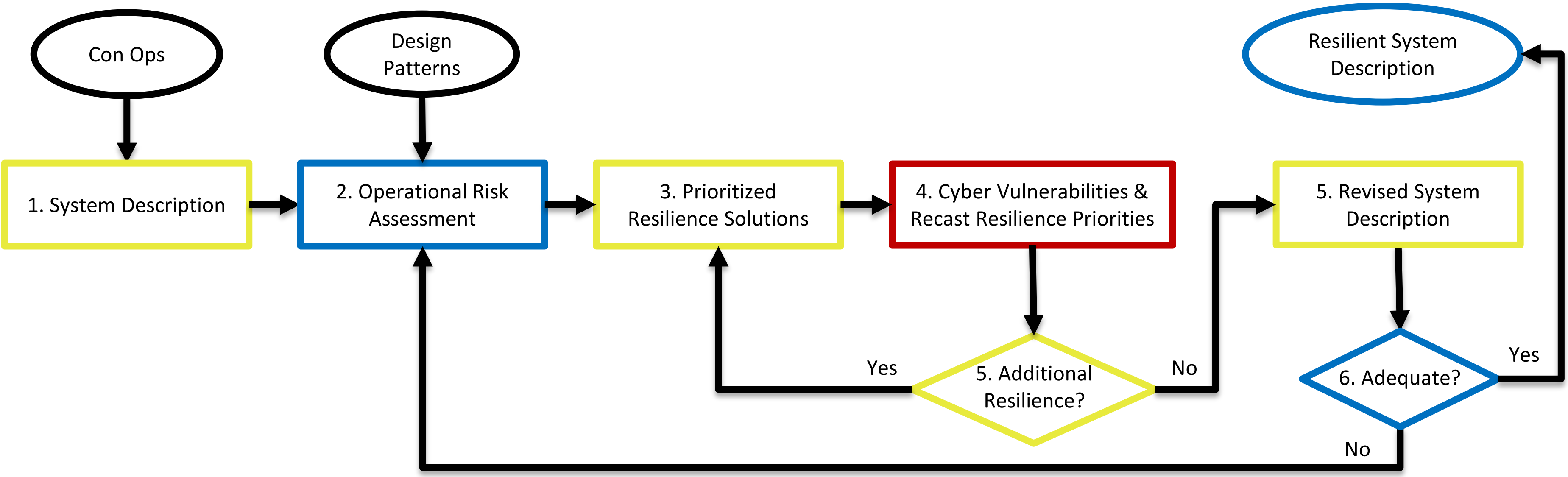
- What to protect and why? Which combination of design patterns to employ in which mission subsystems?

- Who to involve? What information to provide for decision support?
  - —Blue Team: the system/mission owners
    - ○ Provide structured elicitation process from safety community
    - ○ Receive priorities for system functions
  - —Yellow Team: the systems engineers
    - ○ Provide scoping from Blue Team
    - ○ Receive systems models (e.g. SysML)
  - —Red Team: the in-house adversaries
    - ○ Provide systems models and ML tools to cross reference with known attacks
    - ○ Receive vulnerability assessment





Cyber-Security Requirement Methodology (CSRM)


Con Ops
Design Patterns
Resilient System Description
1. System Description
2. Operational Risk Assessment
3. Prioritized Resilience Solutions
4. Cyber Vulnerabilities & Recast Resilience Priorities
5. Revised System Description
Yes
5. Additional Resilience?
No
6. Adequate?
Yes
No

SE Team

Red Team

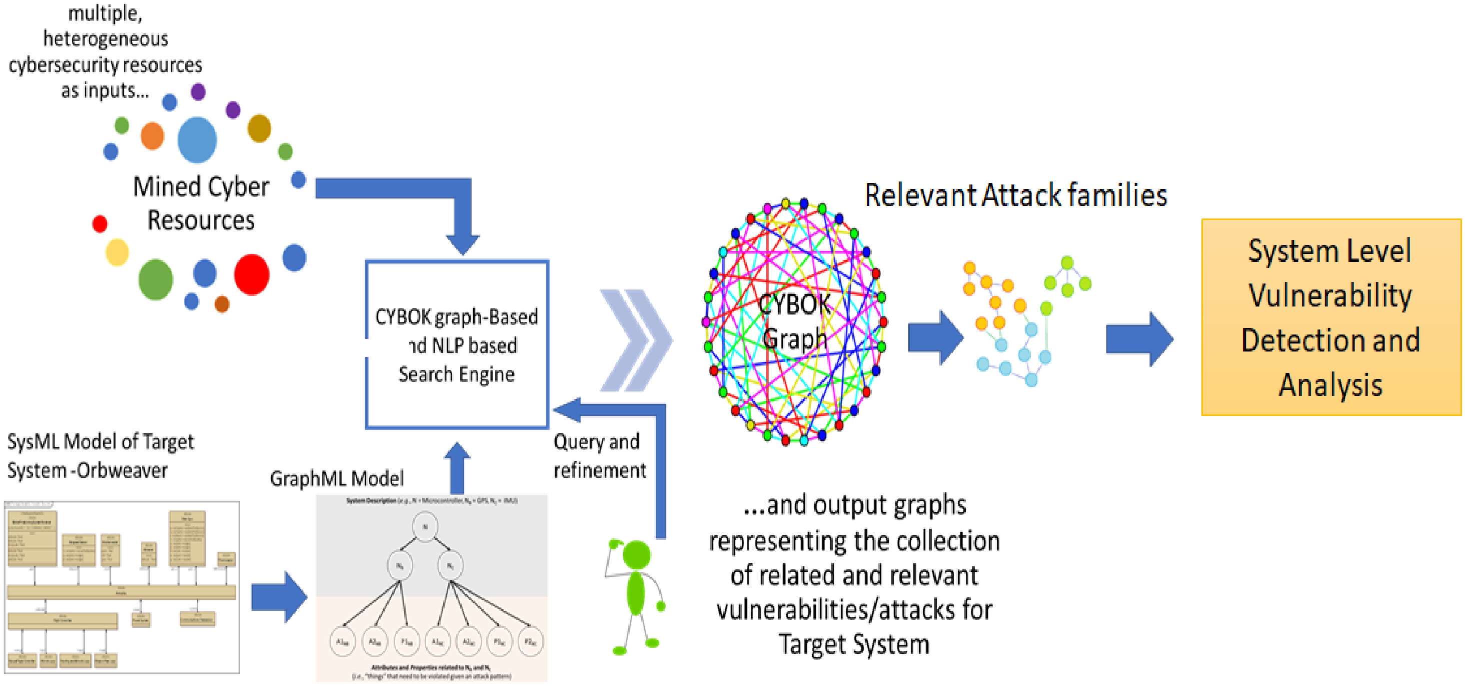
Blue Team

Tools to Support Resilient System Designs

- UVA is currently working with OSD, the Army and the Air Force to develop methodologies and technology to support cyber security design and evaluation
  - —System architectures and reusable SW design patterns for achieving resilience (OSD; RT-142; RT-156, RT-172)
  - —Risk analysis tools for selection of design patterns for specific systems to apply (OSD; RT-156, RT-172, RT-191, RT-196)
  - —Use of SW static analysis tools in concert with dynamic analysis testing (Army; ART-006)
  - —Experiments that address operational processes for achieving resilience and preparation of operators to carry out their roles (Air Force; RT-201)
  - —Resilience requirements methodology (Army; ART-004)

Cyber Body of Knowledge (CYBOK)

- Dr. Carl Elks – VCU
- CYBOK is a multi-view search engine on how to “relate” cyber threat information in a systems model context. It views the diverse set of cyber repositories (CAPEC, CWE, CVE, CPE, etc.) as greater than the sum of their individual parts.
- Uncovering the synergistic relations in these diverse set of repositories and casting the information into “system” model perspective is the innovative aspect of CYBOK.



multiple, heterogeneous cybersecurity resources as inputs...

Mined Cyber Resources

CYBOK graph-Based nd NLP based Search Engine

Relevant Attack families

System Level Vulnerability Detection and Analysis

SysML Model of Target System -Orbweaver

GraphML Model

Query and refinement

...and output graphs representing the collection of related and relevant vulnerabilities/attacks for Target System

CYBOK Graph
System Description (e.g., N = Microcontroller, N1 = GPS, N2 = IMU)
N
N1
N2
Attributes and Properties related to N1 and N2
(i.e., "things" that need to be violated given an attack pattern)

Mission Aware MBSE Meta-Model

Mission Aware (MA) Meta-Model Overview

SysML v2 is proposed standardization target for the formalization of associations between Systems Theoretic Process Analysis (STPA), Model-Based System Engineering (MBSE), and Mission Aware (MA) concepts.

STPA

STPA Handbook
Leveson & Thomas - 2018

MBSE

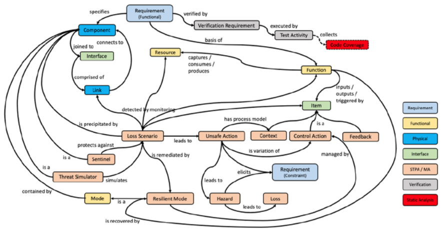
OMG
SysML v2 RFP - 2017

Mission Aware

SERC
2012-2019

MA MBSE Meta-Model

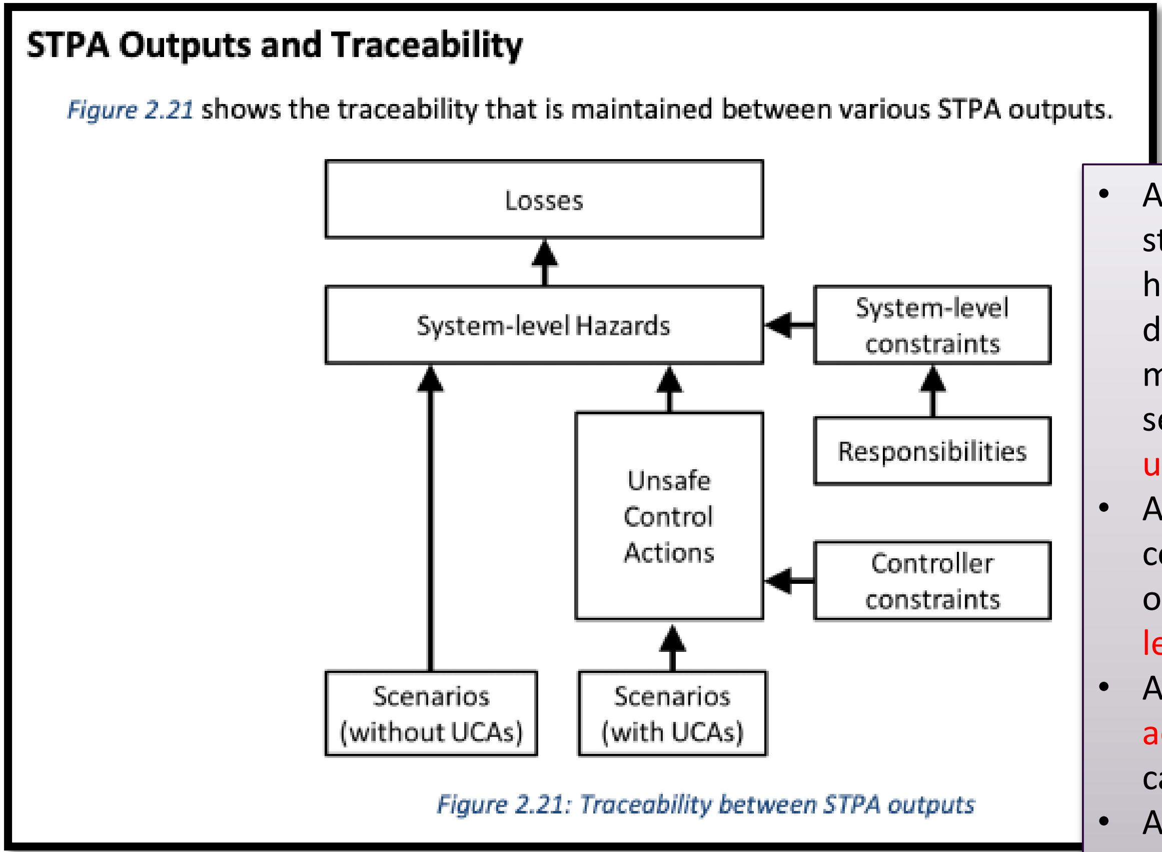
MISSION AWARE



STPA Overview

STPA is an iterative, methodical hazard analysis technique to identify causes of hazardous conditions intended to improve or promote system safety.

- In cyber-physical systems, security can be treated as analogous to safety.



STPA Outputs and Traceability

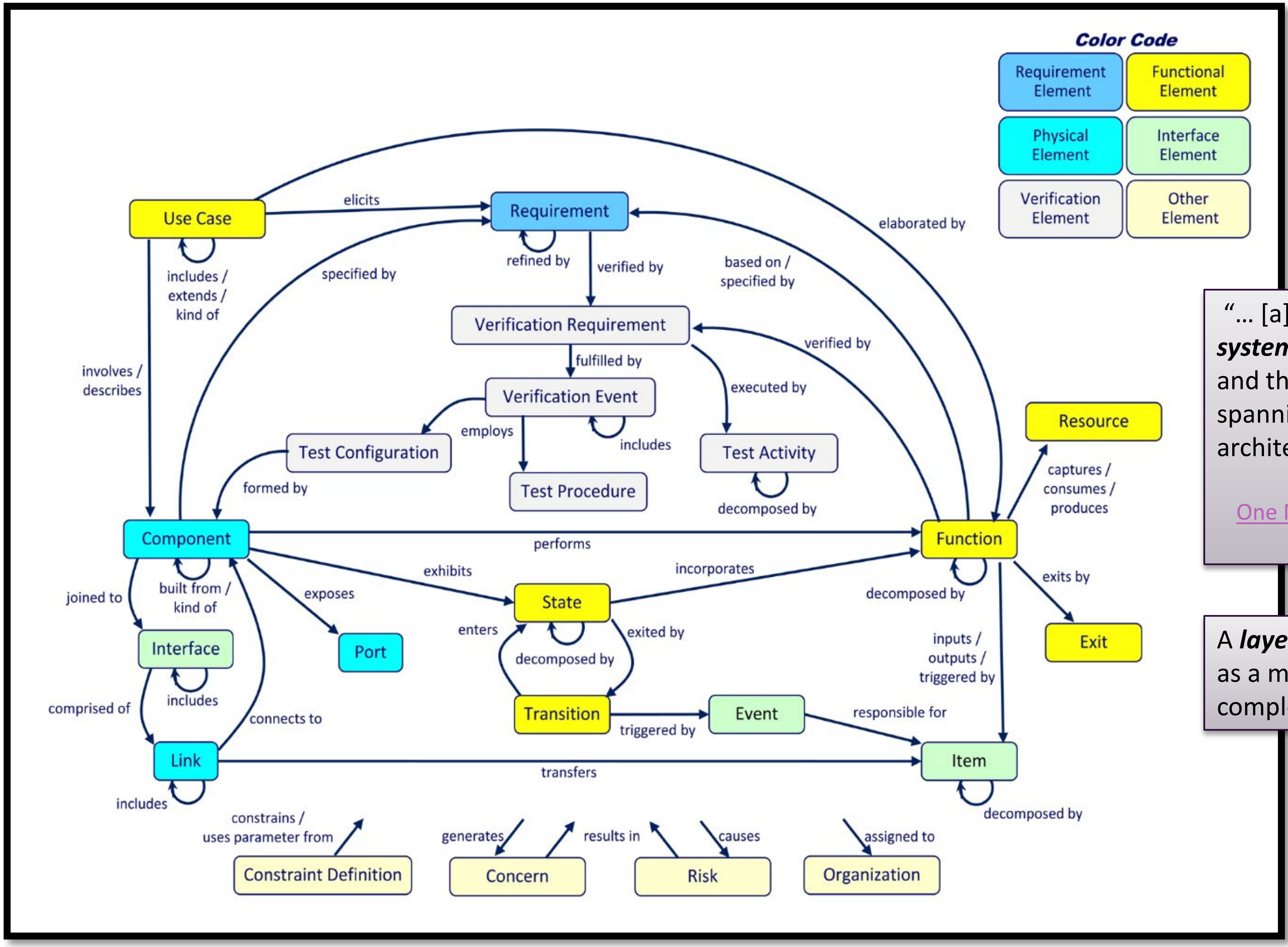
Figure 2.21 shows the traceability that is maintained between various STPA outputs.

Figure 2.21: Traceability between STPA outputs

- A ***Loss*** involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.
- A ***Hazard*** is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.
- An ***Unsafe Control Action*** (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard.
- A ***Loss Scenario*** describes the causal factors that can lead to the unsafe control and to hazards.

MBSE Meta-Model Overview

Key requirement defined by Object Management Group (OMG) for SysML v2 is “*a meta-model of core SE concepts with precise semantics*.” Vitech Corporation MBSE meta-model largely aligns with SysML v2 goals.



“… [a] representation of critical ***systems engineering concepts*** and their ***interrelationships*** spanning requirements, behavior, architecture, and test.”

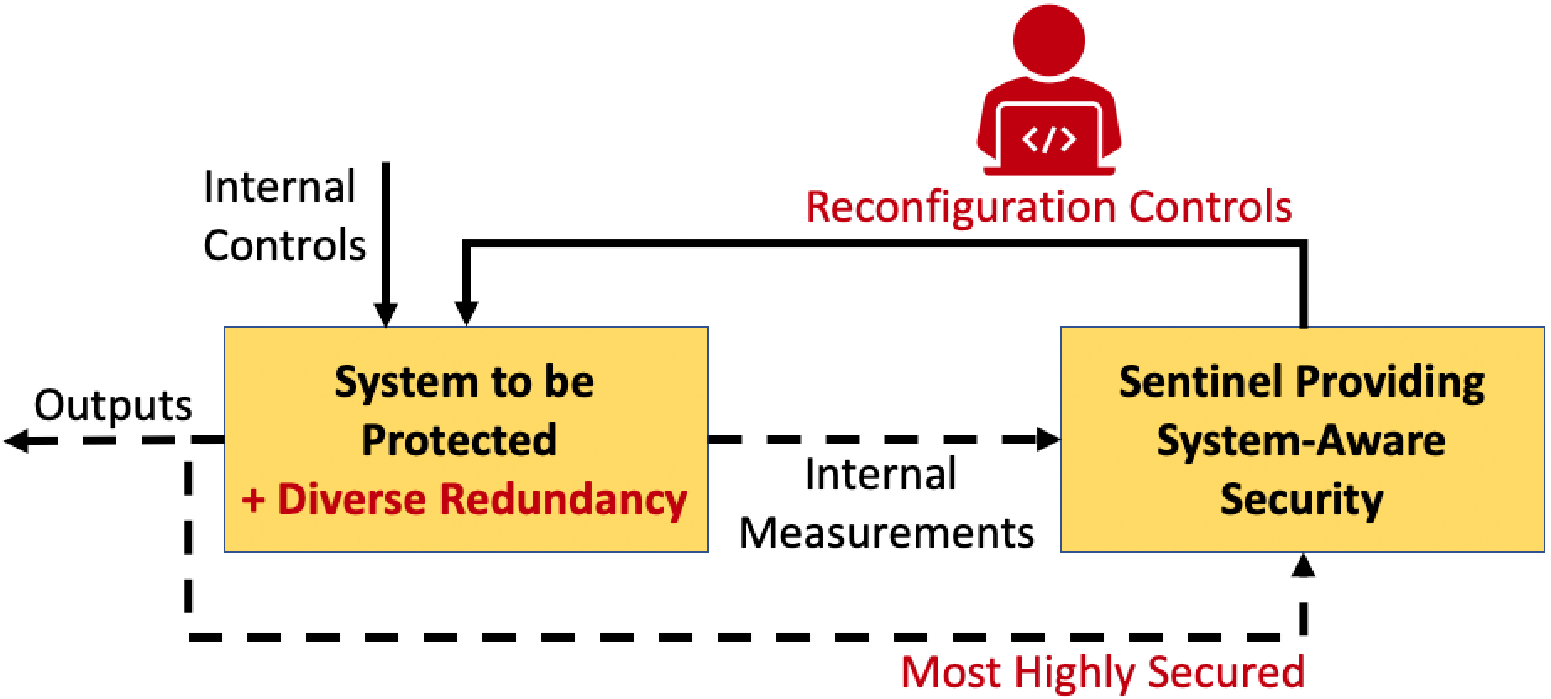
One Model, Many Interests, Many Views - Vitech 2018

A ***layered / hierarchical*** model as a mechanism to manage complexity.

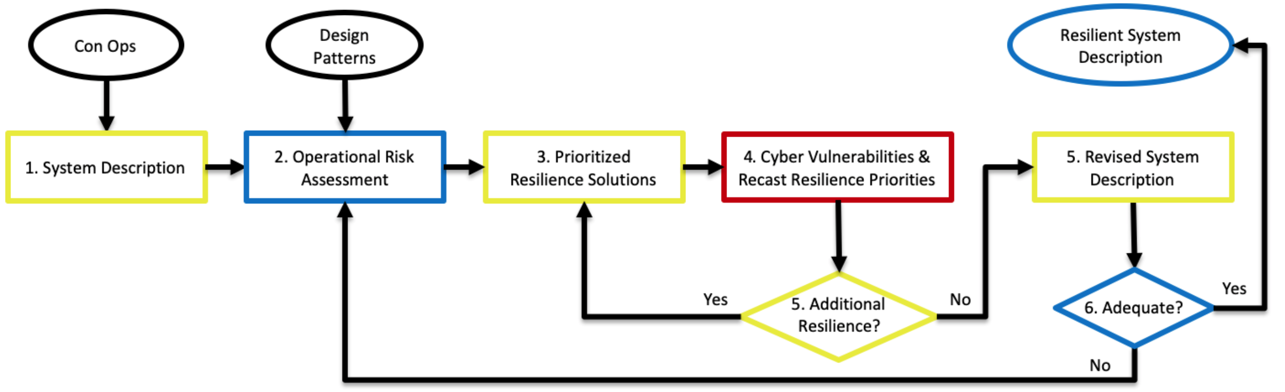
Mission Aware Overview

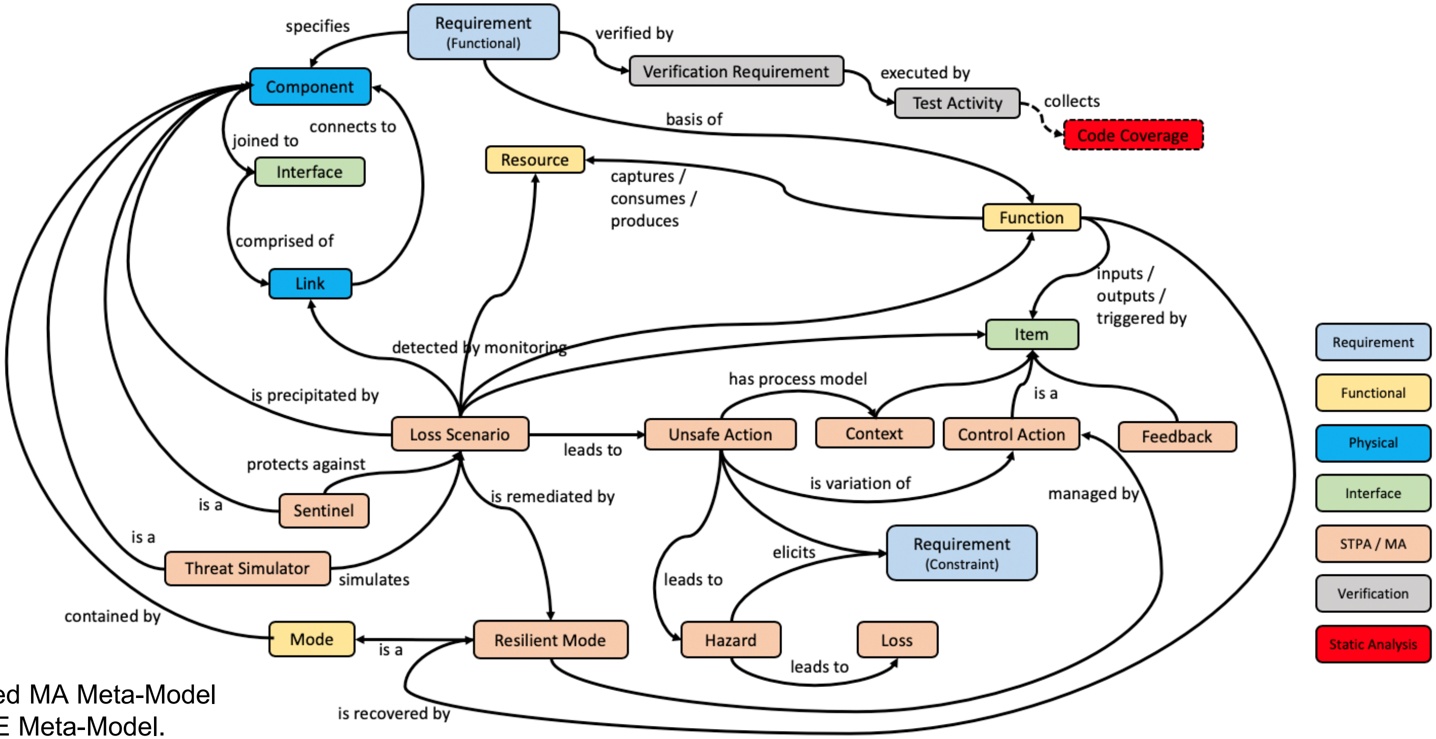
- A ***Resilient Mode*** is a distinct and separate method of operation of a component, device, or system based upon diverse redundancy. Resilience allows the system to maintain a safe level of operational normalcy in response to anomalies, including threats of malicious and unexpected nature.

- A ***Sentinel*** is responsible for monitoring and reconfiguration of a system using available Resilient Modes. The Sentinel subsystem is expected to be far more secure than the system being addressed for resiliency.



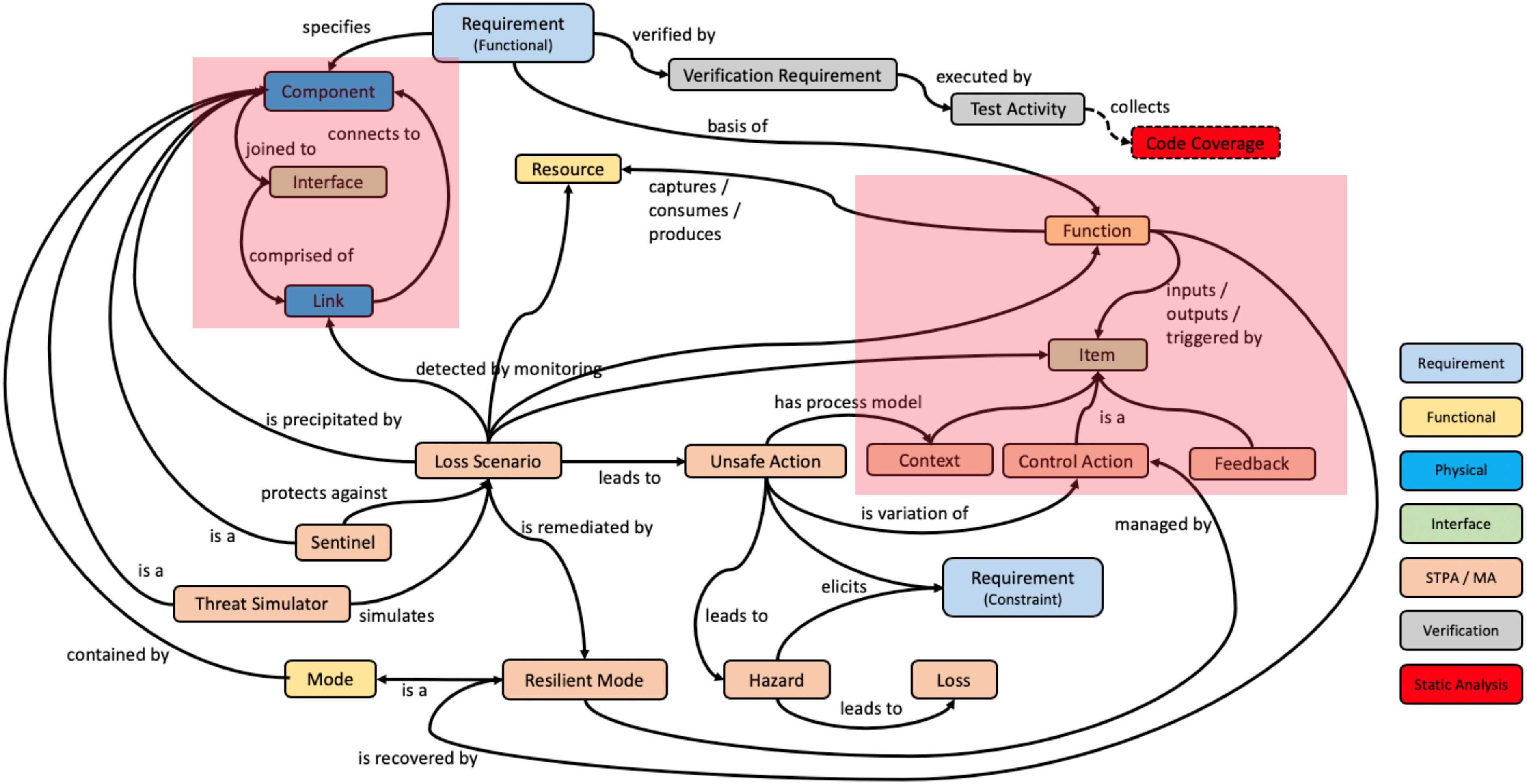
CSRM / MA Meta-Model Mapping


Con Ops
Design Patterns
Resilient System Description
1. System Description
2. Operational Risk Assessment
3. Prioritized Resilience Solutions
4. Cyber Vulnerabilities & Recast Resilience Priorities
5. Revised System Description
Yes
5. Additional Resilience?
No
6. Adequate?
Yes
No

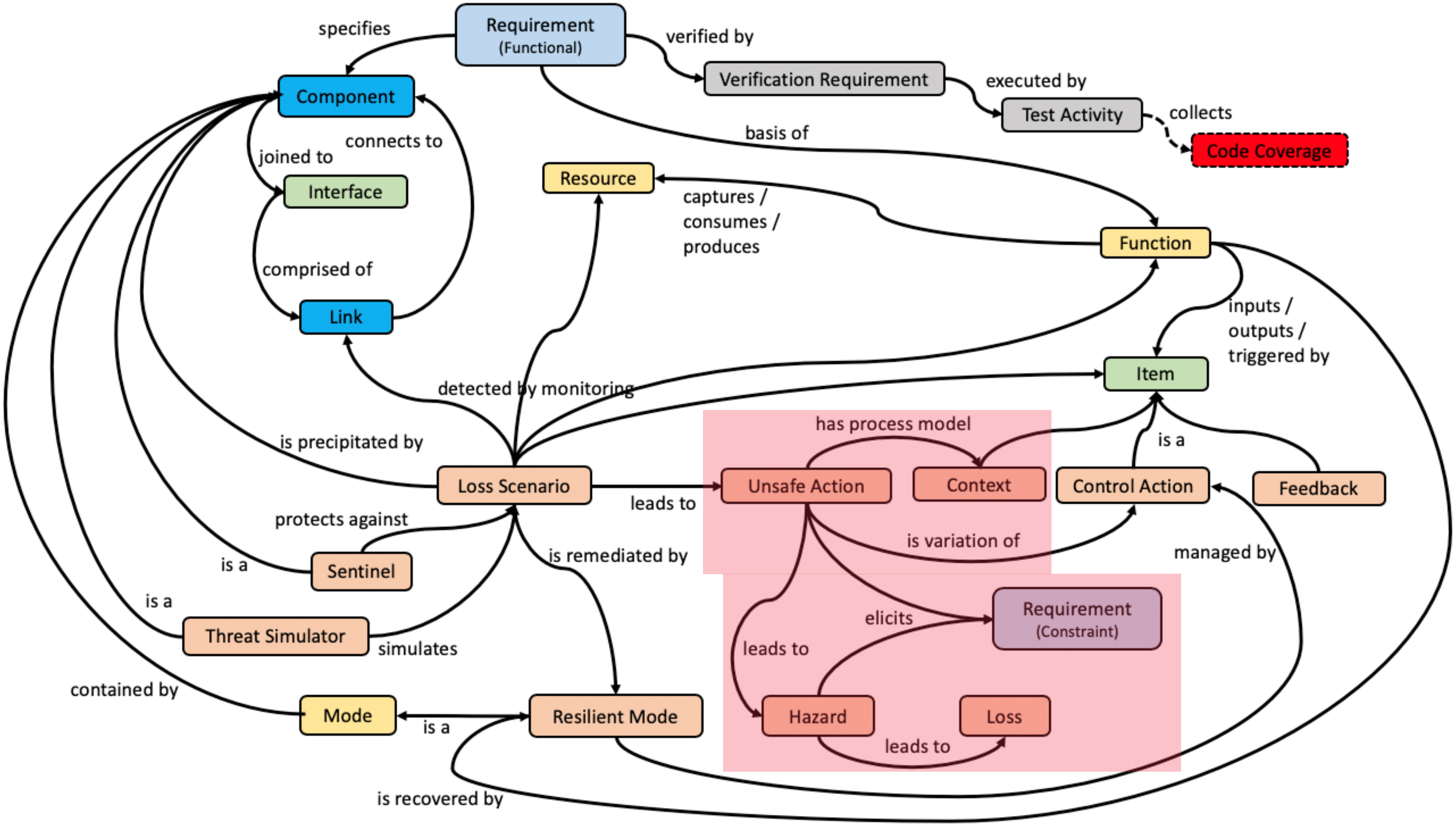


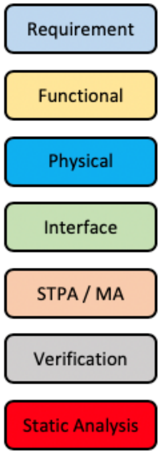
NOTE: For readability, displayed MA Meta-Model includes only a subset of MBSE Meta-Model.

CSRM Step #1 – System Description

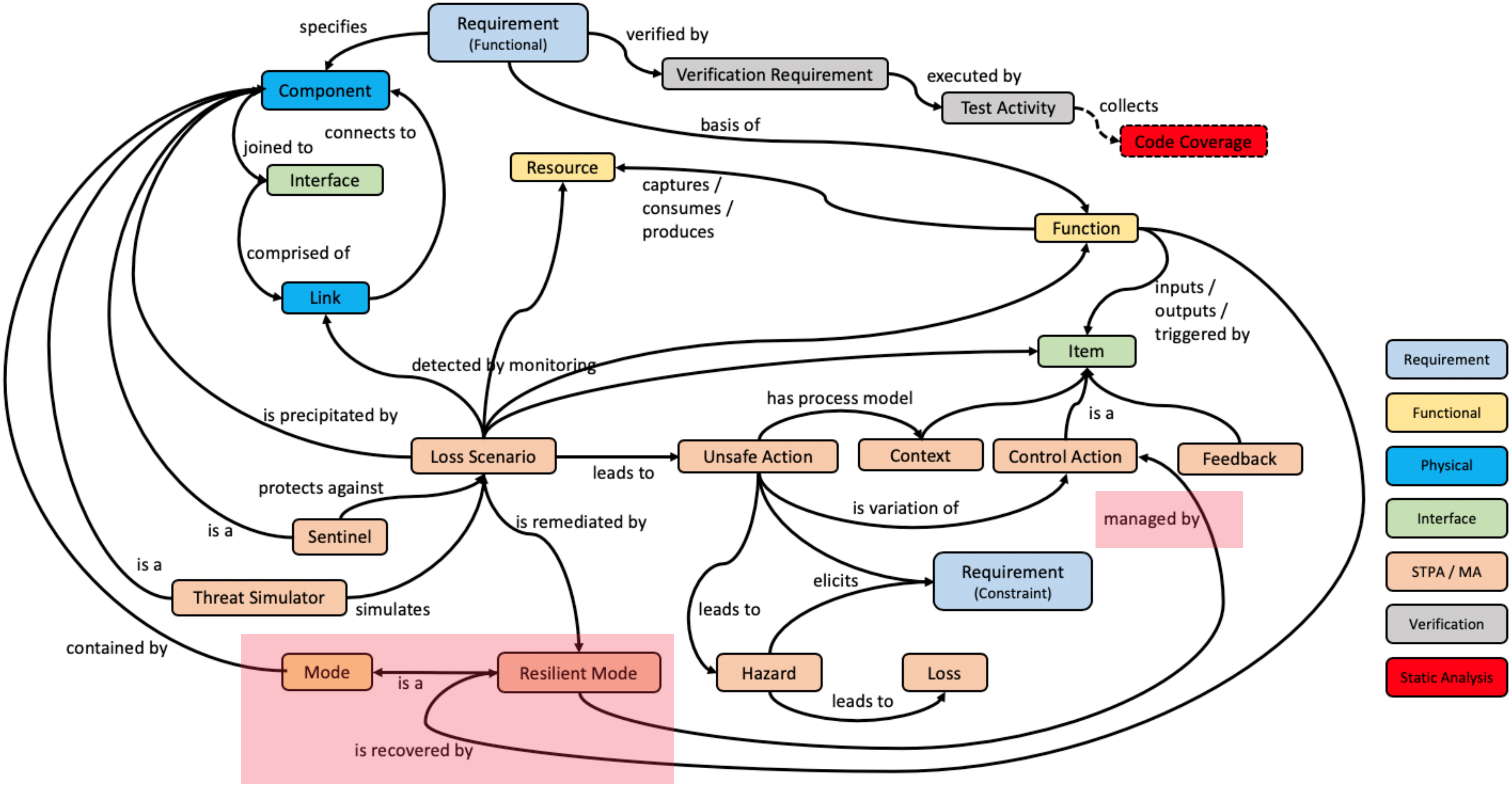


CSRM Step #2: Operational Risk Assessment

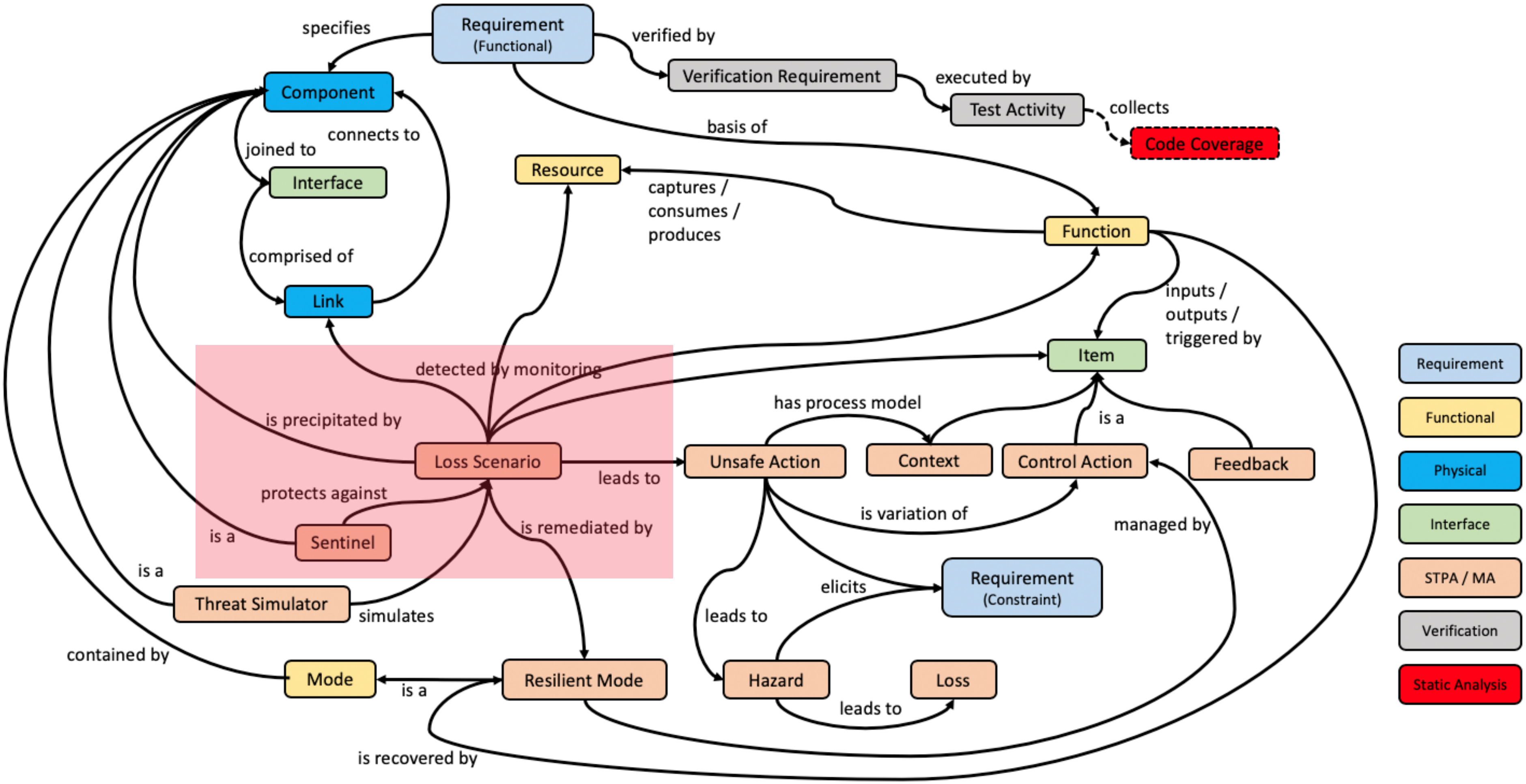




CSRM Step #3: Prioritized Resilient Solutions



CSRM Step #4: Cyber Vulnerabilities & Recast Resilient Priorities



CSRM Step #5/6: Resilience Evaluation

Mission Aware: MBSE Attributes and Metrics

Object	Attribute	Values	Notes
Loss	missionImpact	High / Med / Low	Blue Team
Loss Scenario	attackLikelihood	High / Med / Low	Red Team
	attackType	External Insider SupplyChain	
	attackPattern	<CAPEC-#>:<Title>	
	detectionPattern	DataConsistency ChangingControlInput Introspection	
	detectionTime	seconds	Time budget to detect loss
	isolateTime	seconds	Time budget to isolate loss via system /component tests.
Resilient Mode	complexity	High / Med / Low	Number of model "contained by" associations. Indication of cost.
	effectiveness	High / Med / Low	Impact on remediating High "likelihood" attacks associated with High "mission impact".
	operationalImpact	High / Med / Low	Degree of operator training need. Degree of mission interruption.
	restoreTime	seconds	Time budget to restore system function via resilient mode.
	operatorDecisionTime	seconds	Time budget for operator decision time to enable resilient mode. 0 implies automated resilient mode.

CSRM Step #5/6: Resilience Evaluation

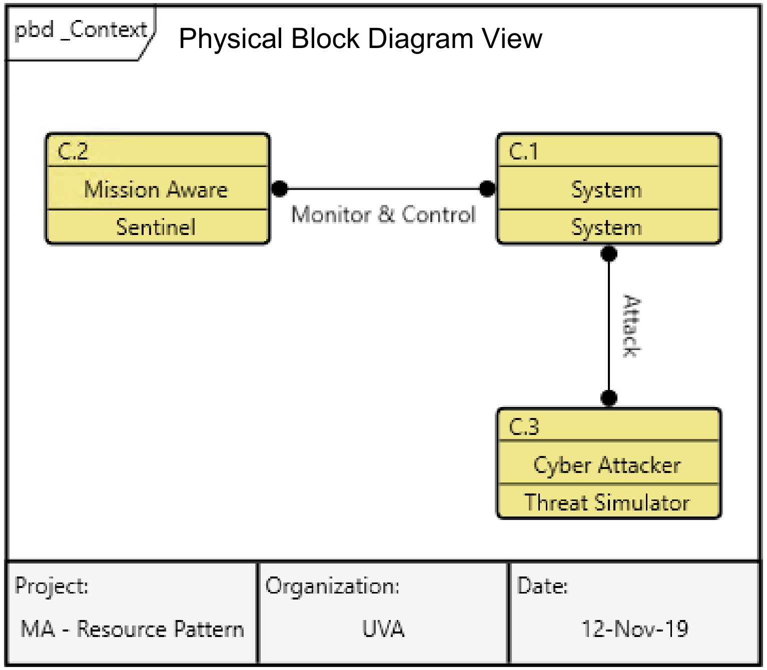
Recovery Ratio: A mechanism to evaluate & refine a System Architecture against defined Resiliency requirements:

- An iterative process as system design is refined / matured

Metric	Units	System Model Evaluation / Simulation
Resilient Mode: “Recovery Ratio” per System Function [per Loss Scenario] *Calculated:* Measured / Expected	< 1: Acceptable > 1: Not Acceptable	Recovery time includes: • Detection • Isolation • Restoration Including: • Technical: System Components • Operational: System-of-System Interactions • Operator: Expected Decision Times
Loss Scenario: Time to Detect	seconds / minutes	Impact tradeoff for Sentinel interfaces: • polling-based (system / link loading) • event-based, etc.
Loss Scenario: Time to Isolate	seconds / minutes	Impact tradeoff for System / Component Test capabilities
Resilient Mode: Time to Restore	seconds / minutes	Impact tradeoff for Resilient Modes: • Active/Active • Active/Standby (Hot / Warm / Cold) Includes Operator decision time

Example: Behavior Model Simulation

Example: Architecture Model



Loss Scenario – Attack Pattern:

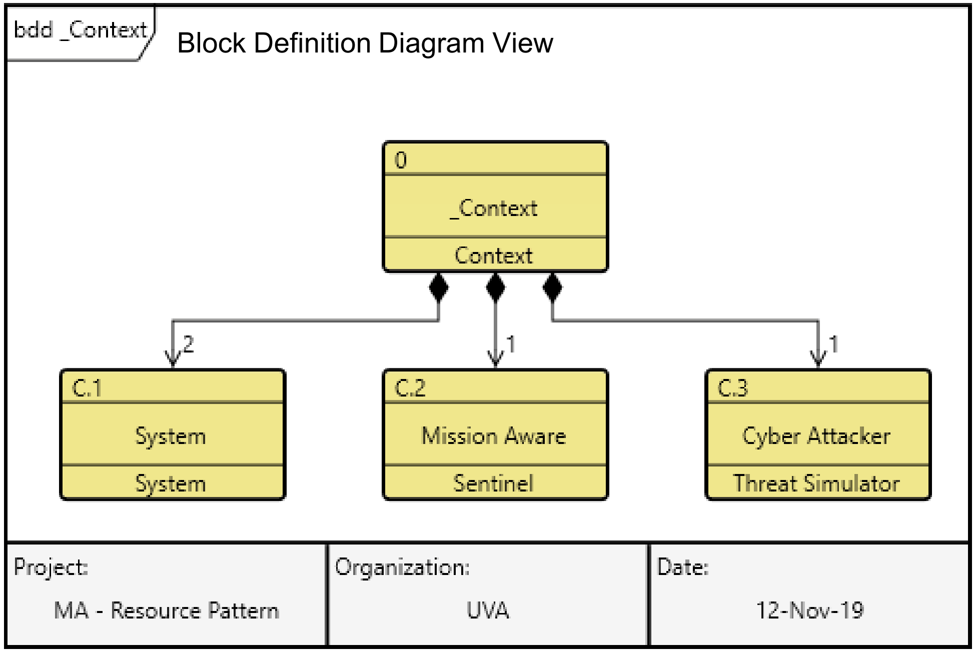
- CPU Overload
- CAPEC-443: Malicious Logic Inserted Into Product Software by Authorized Developer

Sentinel - Design Pattern:

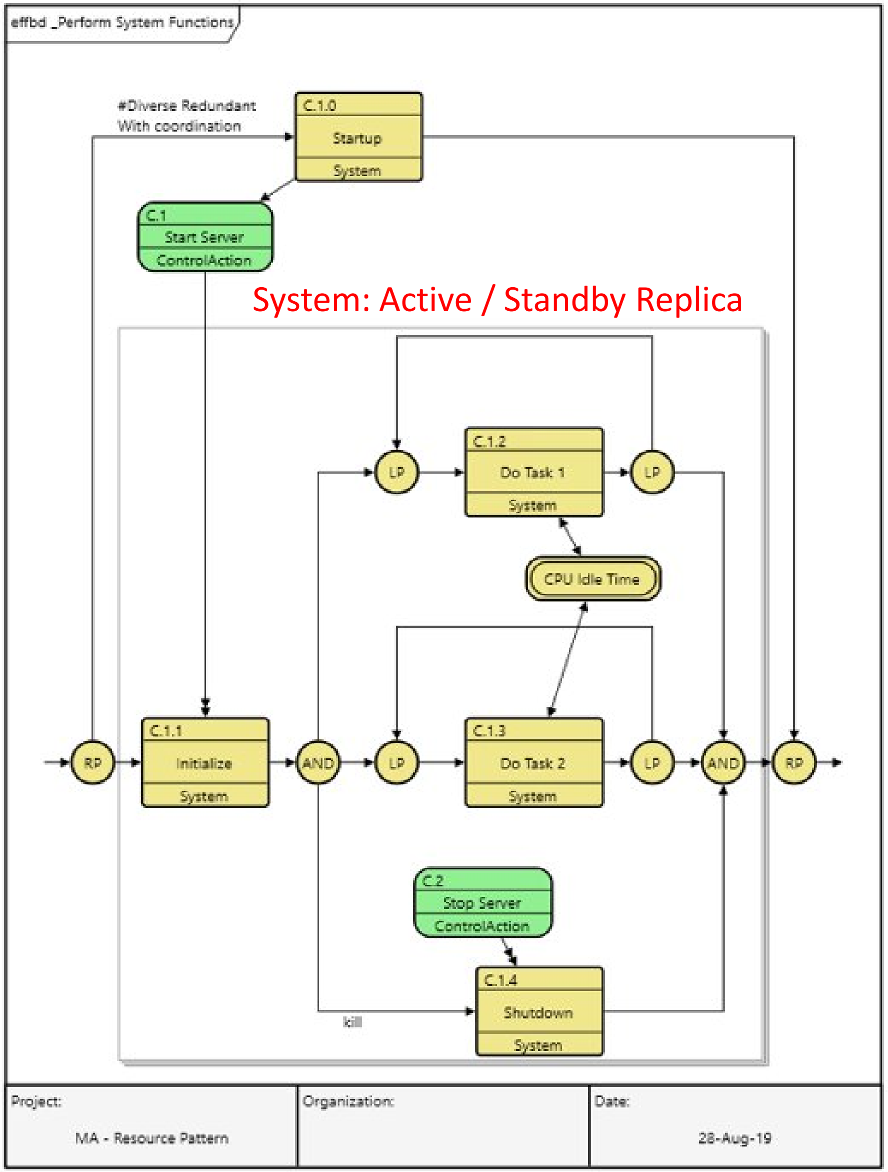
- Resource Introspection - CPU Idle Time

Resilient Mode:

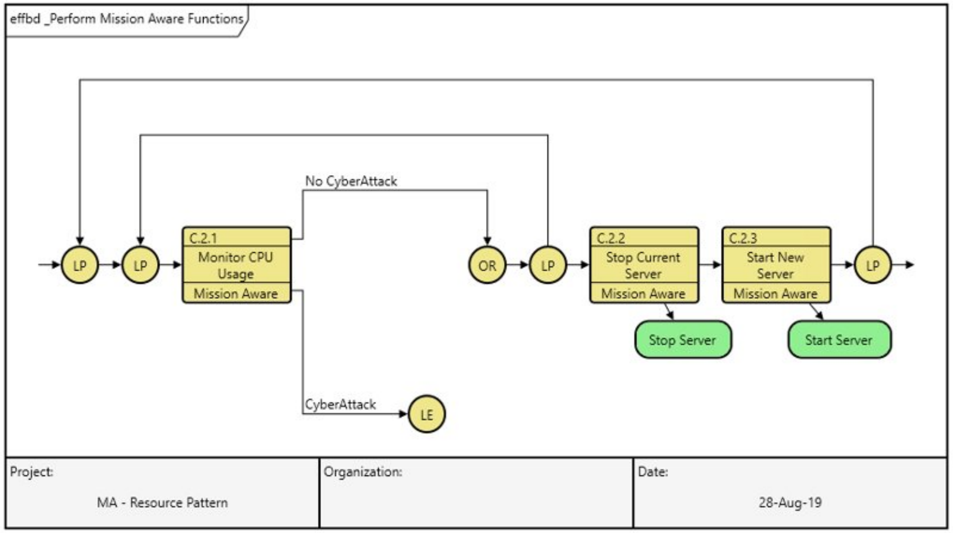
- Active / Standby

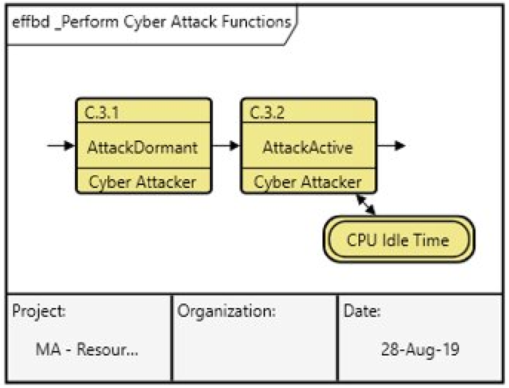


Example: Behavior Model



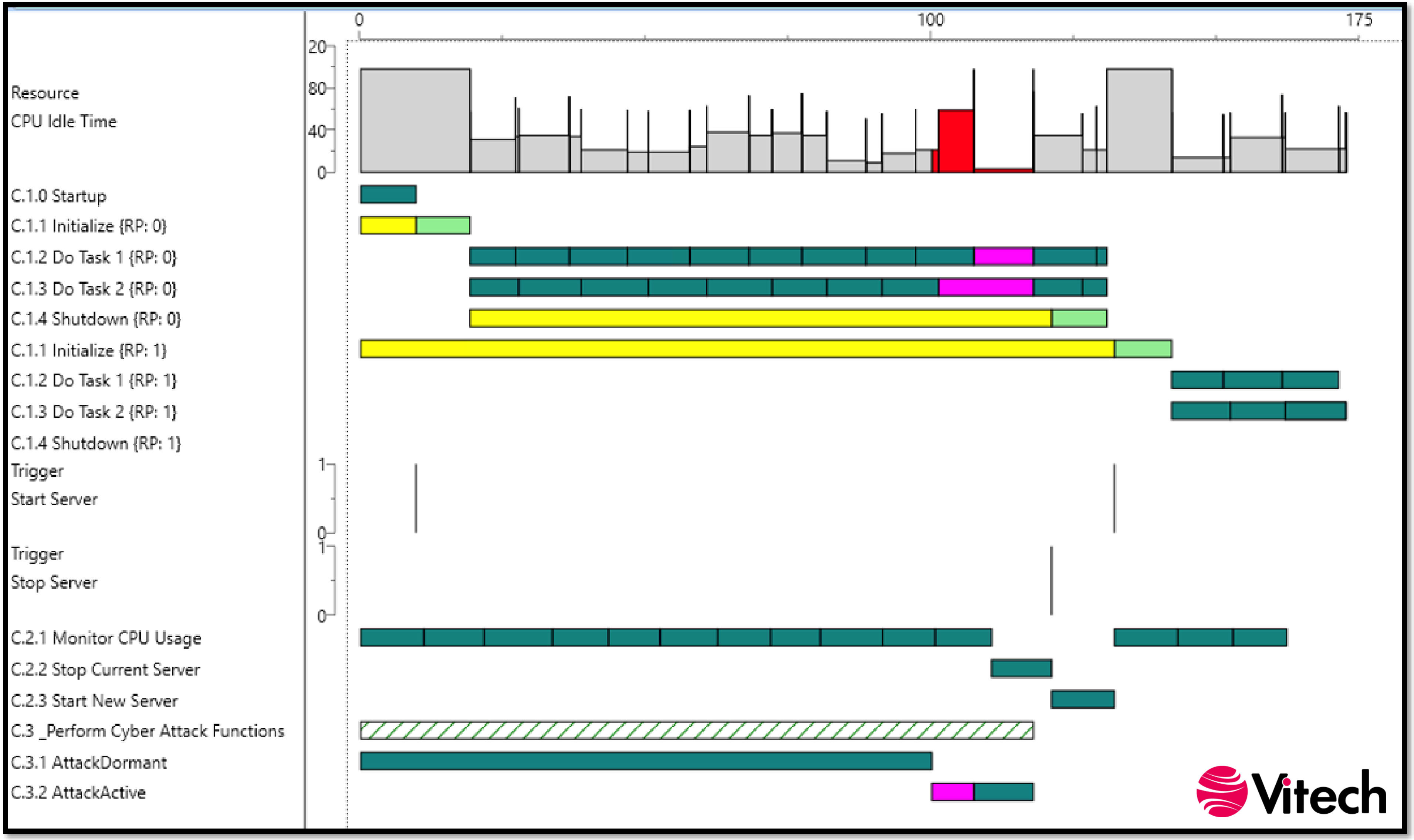
System: Active / Standby Replica





The Enhanced Functional Flow Block Diagram (EFFBD), like its SysML cousin the activity diagram, is a complete representation of behavior. EFFBDs unambiguously represent the *flow of control* through sequencing of functions as well an overlay of *data* and *resource* interactions.

Example: Simulation Transcript



Summary / Additional Research Efforts

Summary / Additional Research Efforts

- Investigation of *GraphQL Schema* as mechanism to publish MA Meta-Model
  - Seamless integration of CYBOK scoring capability
- Refine / validate MA Meta-Model via “Model-Based System Assurance” (ART-004) project
- Additional case studies
  - Silverfish
  - UAVs